# LABORATORY FOR COMMUNICATIONS AND APPLICATIONS LCA

## Secure Neighborhood Discovery in Wireless Networks

Many services offered by wireless networks rely on discovering something about their neighborhood: In routing, a node needs to learn which nodes are available for direct communication; in physical access control, a monitoring system must verify that an access granting token is in physical proximity; in many localization algorithms, a node needs to measure the distance to nearby anchor nodes. However, the open nature of wireless communication make it easy to attack the discovery mechanisms, and thereby abuse the overlaying services. In our work, we investigate the security of neighborhood discovery on various levels: from formal reasoning about cryptographic neighborhood discovery protocols, to attacks on the physical communication layer.

## SECURE NEIGHBOR DISCOVERY

*Neighbor discovery* is the discovery of devices directly reachable for communication or in physical proximity. We elaborate a taxonomy of neighborhood discover protocol properties and a classification of attacks. We provide formal models that allow us to reason about neighbor discovery protocols. We also design neighbor discovery protocols.

- P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux. Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine*, 46(2), 2008
- M. Poturalski, P. Papadimitratos, and J.-P. Hubaux. Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Tokyo, Japan, 2008 [slides]
- M. Poturalski, P. Papadimitratos, and J.-P. Hubaux. Towards Provable Secure Neighbor Discovery in Wireless Networks. In *The 6th ACM Workshop on Formal Methods in Security Engineering*, Alexandria, VA, 2008 [slides]
- R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux. A Low-Cost Secure Neighbor Verification Protocol for Wireless Sensor Networks. In *The 2nd ACM Conference on Wireless Network Security (WiSec)*, Zurich, Switzerland, 2009 [slides]

# SECURE RANGING

*Secure ranging (*also know as *distance bounding)* allows two wireless devices to securely estimate the distance between them, with the guarantee that the estimate is an upper-bound on the actual distance. We explore physical layer attacks on secure ranging, assuming that the underlying physical communication layer is *Impulse Radio Ultra-Wideband (IR-UWB)*. IR-UWB is an emerging technology providing unmatched capabilities of high precision ranging, notably in dense multi-path environments (indoor).

- M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec. Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging. In *3rd ACM Conference on Wireless Network Security (WiSec)*, 2010 [slides]
- M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec. The Cicada Attack: Degradation and Denial of Service in IR Ranging. In *IEEE International Conference on Ultra-Wideband*, 2010 [slides]
- M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec. Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures. *IEEE Transactions on Wireless Communications, 2011*
- M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec. On Secure and Precise IR-UWB Ranging. Accepted to *IEEE Transactions on Wireless Communications, 2012*

# PEOPLE

Prof. Jean-Pierre Hubaux
Marcin Poturalski
Reza Shokri

Collaborators

Prof. David Basin, ETHZ
Prof. Srdjan Capkun, ETHZ
Prof. Jean-Yves Le Boudec, EPFL
Prof. Panagiotis Papadimitratos, KTH